

Aberystwyth University

VisTAS

Ali, Ahmad; Ahmed, Mansoor; Khan, Abid; Anjum, Adeel; Ilyas, Muhammad; Helfert, Markus

Published in:
PeerJ Computer Science

DOI:
[10.7717/PEERJ-CS.516](https://doi.org/10.7717/PEERJ-CS.516)

Publication date:
2021

Citation for published version (APA):

Ali, A., Ahmed, M., Khan, A., Anjum, A., Ilyas, M., & Helfert, M. (2021). VisTAS: Blockchain-based Visible and Trusted Remote Authentication System. *PeerJ Computer Science*, 7, [e516]. <https://doi.org/10.7717/PEERJ-CS.516>

Document License

CC BY

General rights

Copyright and moral rights for the publications made accessible in the Aberystwyth Research Portal (the Institutional Repository) are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Aberystwyth Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Aberystwyth Research Portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

tel: +44 1970 62 2400
email: is@aber.ac.uk

VisTAS: blockchain-based visible and trusted remote authentication system

Ahmad Ali¹, Mansoor Ahmed^{1,2}, Abid Khan³, Adeel Anjum¹,
Muhammad Ilyas⁴ and Markus Helfert²

¹ Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan

² Innovation Value Institute, Maynooth University, Maynooth, Ireland

³ Department of Computer Science, Aberystwyth University, Aberystwyth, United Kingdom

⁴ Department of Computer Science and IT, University of Sargodha, Sargodha, Pakistan

ABSTRACT

The information security domain focuses on security needs at all levels in a computing environment in either the Internet of Things, Cloud Computing, Cloud of Things, or any other implementation. Data, devices, services, or applications and communication are required to be protected and provided by information security shields at all levels and in all working states. Remote authentication is required to perform different administrative operations in an information system, and Administrators have full access to the system and may pose insider threats. Superusers and administrators are the most trusted persons in an organisation. “Trust but verify” is an approach to have an eye on the superusers and administrators. Distributed ledger technology (Blockchain-based data storage) is an immutable data storage scheme and provides a built-in facility to share statistics among peers. Distributed ledgers are proposed to provide visible security and non-repudiation, which securely records administrators’ authentications requests. The presence of security, privacy, and accountability measures establish trust among its stakeholders. Securing information in an electronic data processing system is challenging, i.e., providing services and access control for the resources to only legitimate users. Authentication plays a vital role in systems’ security; therefore, authentication and identity management are the key subjects to provide information security services. The leading cause of information security breaches is the failure of identity management/authentication systems and insider threats. In this regard, visible security measures have more deterrence than other schemes. In this paper, an authentication scheme, “VisTAS,” has been introduced, which provides visible security and trusted authentication services to the tenants and keeps the records in the blockchain.

Submitted 3 March 2021

Accepted 8 April 2021

Published 12 May 2021

Corresponding author

Ahmad Ali,

enr.ahmadali@yahoo.com

Academic editor

Mamoun Alazab

Additional Information and
Declarations can be found on
page 22

DOI 10.7717/peerj-cs.516

© Copyright

2021 Ali et al.

Distributed under

Creative Commons CC-BY 4.0

OPEN ACCESS

Subjects Computer Networks and Communications, Cryptography, Distributed and Parallel Computing, Security and Privacy, Operating Systems

Keywords Deterrence, Secure authentication, Supervised authentication, Insider threats, Cryptography, Web and internet services, Data science, Databases, Security & privacy

INTRODUCTION

Authentication plays a vital role and depends on the prominence and significance of assets or resources that are being secured. Basic information systems security can be provided by implementing essential features of confidentiality, integrity, and availability (Sicari et al., 2015; Farooq et al., 2015; Kumar, Veale & Srivastava, 2016). Implementation

of managed and meticulously supervised access to its clients is the essential requirement for the security of an information system ([Barrera et al., 2017](#)). After the qualifying conditions of physical access control, next is the electronic authentication to be conducted.

Various methods are required on different IoT layers to cope with the authentication requirements in the Internet of Things (IoT). Three main layers of authentication are the system, application or program, and the users. Different architectures and policies can be implemented to accomplish IoT devices' individuality and stop cloning the machines. The idea of using intrinsic physical characteristics of identification devices is Physical Un-clone-able Functions (PUF). This principle includes physical features at the hardware level to restrict and safeguard the device from cloning issues. Another strategy for the user or device authentication is dongle-based paired computers. Encryption schemes are incorporated in Secure authentication, which is either symmetric or asymmetric. Crossman et al. ([Crossman & Liu, 2015](#)) also recommended the use of encryption for authentication credentials as well as digital certificates issued by a Public Key Infrastructure (PKI) for secure system authentication. Similarly, the application's authentication is accomplished using digital certificates, which is the primary solution for implementing application authentication ([Markmann, Schmidt & Wählisch, 2015](#)). After system authentication and application authentication, the authentication of users to determine their legitimacy is involved. Researchers from time-to-time have suggested different methods to minimise insider vulnerability. Most of the methods suggested the assessment and review of behavioural changes and psychological effects of the insiders. Some researchers proposed an analysis of social activities. Technical controls in this context were lacking except log analysis and tracking user activities. The Common Sense Guide and to Mitigating Insider Threats in all nations by SEI (Information Engineering Institute) provides comprehensive guidance to reduce insider threats ([Silowash et al., 2012](#); [Flynn et al., 2013](#)). Another guide to mitigating insider risks is the Worst Practices guide by Matthew Bunn and Scott D. Sagan, who have outlined certain practices that did not prove successful ([Bunn & Sagan, 2017](#)). Various authentication schemes are used for the authenticity of a user. The following section will discuss threats & vulnerabilities, authentication procedures, and various authentication schemes.

Temporal variables are additional parameters for authentication security. (i) Something you know (ii) something you have and (iii) something you are, are some known identification variables. Similarly, temporal variables to constraint an individual are (i) only for Identified User, (ii) only for Specified Time, and (iii) only at specified Geo-Location ([Ali et al., 2020](#)).

Multiple types and methods are used to provide user authentication, e.g., one factor uses user ID and password. The 2nd factor is used for additional security, such as verification of authentication via SMS, use of biometric devices, passcode via email, or even using a phone call or any other appropriate multi-factor authentication schemes. The 3rd element for secure authentication is the use of encryption techniques in the transfer of credentials. Credit/Debit Card Transactions are validated by a three-dimensional (3D) authentication, which depends on another party for a secure authentication approach. In the delivery of secure authentication, smart cards often play a significant role. Users can be identified and

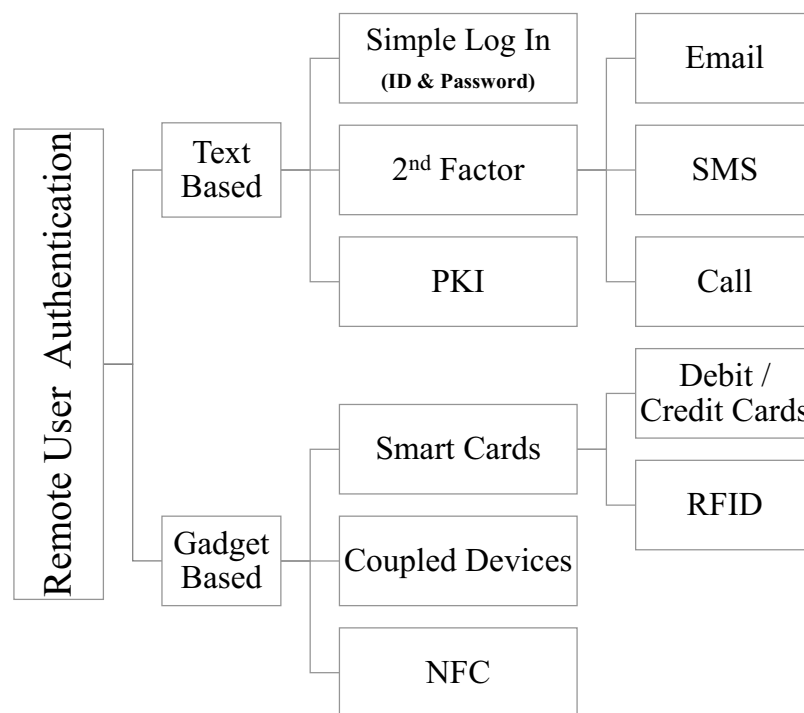



Figure 1 Remote user authentication—taxonomy.

Full-size  DOI: [10.7717/peerj-cs.516/fig-1](https://doi.org/10.7717/peerj-cs.516/fig-1)

authenticated remotely by various methods as shown in Fig. 1. A detailed taxonomy as developed in Ali et al. (2020) covers various other authentication schemes.

- Text-based authentication, which uses textual input (user identification and password), which may include Multi-factor Authentication using SMS, email, etc., also).
- 3rd dimensional (the other party guaranty is essential for transactions on financial cards).
- Biometrics (human body sensors like fingerprints, voice signatures, retina scans, and other wearable sensors).
- Coupled dongles (devices like electronic gadgets etc.).

We need to concentrate not just on identification by recognition but also on verification and authentication of each operation and transaction in terms of financial services and other sensitive environments. IoT operating system based centralised authentication is another concept to allow access control. The growth, availability, and application of these newly introduced operating systems would dramatically improve IoT users' confidence. The WoT operating system would also increase users' trust in WoT, i.e., IoT scalability, to a higher degree. Users belong to various set-ups and are granted varying types of access permissions (Ahmad et al., 2016).

Distributed ledger technology's advantages

A blockchain is a distributed ledger composed of blocks that are linked with the help of cryptography. Each block is made up of a sequence of transactions. To secure the entire chain of these blocks, each one is linked to its predecessor using a cryptographic hash. Even

in a decentralised environment, data stored in a blockchain can be verified, leading to a wide range of blockchain applications. [Chowdhury et al. \(2019\)](#) and [Deepa et al. \(2020\)](#) have presented a comparative analysis that reviews the viability, approaches and opportunities of the well-established DLT platforms, both private and public. Anyone can change the state of a public ledger (Permissionless Ledger) by storing new blocks and updating data through transactions between participating entities. In contrast, only authorised and trusted entities can participate in transactions on a private ledger (Permissioned Ledger), ensuring that the ledger's data is kept private. Smart contracts are used to keep transaction processes secure and traceable ([Bhardwaj et al., 2020](#)). Multiple mission-critical applications have implemented blockchain-based secure data delivery and storage as discussed by [Bera et al. \(2020\)](#) and [Ali et al. \(2021\)](#). The benefits and mechanism of data storage in the blockchain is discussed by [Wang et al. \(2020\)](#). Along with the advantages of blockchains, this technology is not yet mature enough to handle security, privacy and management issues completely, as highlighted by [Singh et al. \(2020\)](#) and [Singh, Hosen & Yoon \(2021\)](#).

Motivation

Trust measurement and incident monitoring are used to perform trust evaluations. Computing environments are very dynamic and versatile in nature. Hardware, Software, Databases, and Communication threats collectively pose to IoT environment as highlighted by [Bou-Harb et al. \(2017\)](#); [Fischer \(2014\)](#) and [Langner, 2011](#); [Masdari & Ahmadzadeh \(2017\)](#). Multidimensional threats have been reported that pose to Security and Privacy separately and Trust in IoT as a whole. A taxonomy of basic security threats is explained by [Jouini, Rabai & Aissa \(2014\)](#). Most Information Technology infrastructure components are vulnerable to a wide range of threats ([Bisong & Rahman, 2011](#); [Kandias, Virvilis & Gritzalis, 2011](#); [Schlicher, MacIntyre & Abercrombie, 2016](#)). These can be categorised into external or outsider threats as well as internal threats or insider threats.

- **Outsiders Threat:** Also known as External Threat. A threat originating from outside of a company, government agency, or institution [Jouini, Rabai & Aissa \(2014\)](#).
- **Insiders Threat:** This is also known as the inner threat or internal threat. Threat originating within a company, government agency, or institution and typically exploited by a disgruntled employee denied promotion or informed of the termination of employment ([Jouini, Rabai & Aissa, 2014](#)). Insiders could have direct access to the organization's ICT infrastructure and can exploit the vulnerabilities, and may have escalated privileges by breaching the information protection control system ([Yusop & Abawajy \(2014\)](#)).

Ivan Homoliak has conducted a state-of-the-art survey ([Homoliak et al., 2019](#)) and compiled all the available dimensions of insider threats and defence solutions in this category. Though different types and factors-based authentication schemes have been proposed, as summarised in [Table 1](#), all of them have limitations to provide supervised authentication, peer control, visible access, storage of immutable login information, and deterrence.

Table 1 Authentication types.

| Sr. No | Factor(s) | Initial Parameters | Mutual Authentication | Applicability | Attacks Covered | Vulnerabilities | Threats | Model | Vulnerabilities |
|--|-----------|--|-----------------------|---|---|--|---|--|--|
| 1 | 1FA | User ID & Password | No | Very easy and user friendly | Open Access, Basic Identity | Multiple | Multiple | Simple Login Form | One Time ID/ Password may be guessed/cracked |
| 2 | | Use of Biometric Authentication | No | Difficult, Biometric devices are not available anywhere | Social engineering/ dictionary | NO | NO | Finger Print Readers | Online Systems are not matured enough |
| 3 | | Use of wearable sensors (ECG, EEG) | No | Difficult, Devices are not available anywhere | Social engineering/ dictionary | NO | NO | Medical Gadgets | Online Systems are not matured enough |
| 4 | | Voice signatures | Yes | Difficult, Devices are not available anywhere | Social engineering/ dictionary | Voice Signature Reproduction | Yes | Google Voice, Nuance etc. | Recorded data can be reproduced easily |
| 5 | 2FA | User ID & Password, Email is used for 2FA | Yes | Very easy and user friendly | User Identification & Mutual Authentication | Email Spams | Email may already Compromised | Financial Transactions | If email account is already compromised |
| 6 | | User ID & Password, Mobile Phone is used for 2FA | Yes | Very easy and user friendly | User Identification & Mutual Authentication | Smart Phone Vulnerabilities | Phone may already Compromised | Email Services like Gmail | If Mobile Phone is already compromised |
| 7 | | User ID & Password, USB is used for 2FA | Yes | Very easy and user friendly | User Identification & Mutual Authentication | Smart Phone Vulnerabilities | Phone may already Compromised | Gmail USB Dongle based Authentication Services | What if USB Dongle Got Lost/ Cloned |
| 8 | 3FA | User ID & Password, Email is used for 2FA, Symmetric encryption to avoid spams is incorporated | Yes | Easy, but technically depends on user skill level | User Identification & Mutual Authentication | Key Compromises | – | Custom Build Authentication Frameworks. e.g., WebSeA | If any of the factor source/services are not available |
| 9 | | User ID & Password, Email is used for 2FA, Asymmetric encryption is incorporated | Yes | Technically depends on user skill level | Non-repudiation | Certificate may Lost | – | Custom Build Authentication Frameworks. e.g., WebSeA | If any of the factor source/services are not available |
| 10 | 3D | 3rd party acts as intermediary | Yes | Requires trust among parties | Non-repudiation | International laws may not be effective | | International joint Ventures like VISA and Master | A Central DRU (Dispute Resolution Unit) Acts to resolve the issues |
| Additional Authentication Factors (AF) | | | | | | | | | |
| 11 | 4th AF | Geo Location parameter | Yes | Not applicable for indoor activities | – | Services may not be available everywhere | IP Based Location Tracking | EBSCO Services (SANS Patent) | IP Cloning/ Spoofing etc. |
| 12 | 5th AF | Voice signatures | No | Easy, but technically depends on user skill level | – | Recorded data can be reproduced easily | Sound may vary due to weather and may be reproduced | Google Voice, Nuance etc | |

Contribution

Insider threat is a fundamental and important cause of data breaches. A Russian proverb has fascinating stories about the USA—Russia relationships as “Trust, but Verify” [Markóczy \(2003\)](#). Some psychologists counter it as “Distrust and vilify”, a totally different approach. A sharp liner difference exists between vigilance and distrust, i.e., both are very different.

Whereas, to develop mechanisms that can protect systems from such insider threats, we have to reconsider the importance of vigilance ([Markóczy, 2003](#)). Institutes engage employees because they have trust in them. Identification and authentication mechanisms focus on user input, but ID theft and password leakage, social engineering are common practices in people with malicious intentions. In this paper, we have proposed a visible monitoring system to mitigate insider threats. Physical, logical, and social levels should be considered to analyse the insider threat holistically to prevent, detect and recover from these attacks. Our primary focus is on how to allow privileged users to perform valid/legitimate activities only. Other layers of information security should also be considered carefully. The contribution and research questions are as under.

Research Questions: A generic information security system is supposed to provide deterrence against miscreants’ attempts, prevent and protect from their attacks, timely detect such attempts and finally provide remedies against such detected abusive acts. Validation of any transaction in Information System Management operations/activities is critical and will enhance the system security exponentially ([Theoharidou et al., 2005](#)). Identity management and authentication schemes are the core area of a secure information system. Though different types and factors based authentication schemes are present, as discussed earlier but all of them failed to provide supervised authentication, peer control, visible access, and deterrence ([Homoliak et al., 2019](#)). Research questions have been formulated after a comprehensive literature survey, and “Deterrence” is found as the only research area left behind which needs more focus.

1. How to achieve deterrence in information security (Fear of being caught red-handed)?
2. How to provide visibility in an authentication scheme?
3. How to achieve peers confidence for better trust?

This paper has proposed a deterrence-based authentication system in which authentication is carried out in a peer review and visible to the stale holders. The login requests are recorded in a distributed ledger and shared among registered peers.

Related work concerning authentication schemes is covered in “Related Work”. Highlights of contribution of this paper is given in “Contribution” and proposed authentication system (VisTAS) is covered in “The Proposed Model—VisTAS”. The performance and results of the proposed system are explained in “Results & Discussion”. SWOT analysis containing Strengths, weaknesses, opportunities, threats, a summary of results and discussion of the proposed model have been covered in “Swot Analysis”, and the paper is finally concluded in “Conclusion and Future Work”.

RELATED WORK

Electronic authentication evolution is revolutionary and has reached the current state through several improvements to provide security to the resources. With the advent of technology and hacktivism, the initial text-based single-factor authentication scheme could not meet the information security requirements. This led to the development of two-factor authentication and further progress in using multi-factor encryption and coupled devices. Wang et al. [Wang et al. \(2015\)](#) published a systematic study of two-factor authentication in which authors have posed concerns and weaknesses in the two-factor authentication mechanism and showed uncontrollable issues with the functional manifestation of adversary resources. Since the introduction of two-factor authentication, the usage of coupled sensors has been implemented. Van der Haar et al. studied the critical implementation of the recursive utility of smart devices. IoT requires authentication for the protection, services, and advantages of utilising wearable sensors to authenticate individuals protected by this article. IoT is recursively applied, e.g., IoT also requires authorisation as these are required for the authentication of wearable sensors ([van der Haar, 2015](#)). Munch-Ellingsen et al. boosted their opinion of 2nd factor authentication by utilising coupled/hardware-based authentication. Cipurse contactless cards were initially developed to satisfy the transport industry's needs, and the first iterations of the specification were mirrored and followed by the Open Standard for Public Transport (OSPT) Alliance. Since smartphones are mainly Bluetooth-enabled, Bluetooth-based devices are proposed to monitor smartphones as coupled devices ([Jeong et al., 2015](#)). Host Card Emulation (HCE) and Close Field Contact (NFC) are the two aspects of smartphone-based authentication. They have a single element of IoT authentication. The writers have illustrated the limitations and abuse of these functions.

An additional SMS service solution was proposed as a 2nd factor ([Munch-Ellingsen et al., 2015](#)) authentication to fix these flaws. The user's security and data privacy risks are outlined in Jacobsson's home automation systems and explored in the Smart Homes ([Jacobsson, Boldt & Carlsson, 2015](#)) realm. All the research culminated on the importance of integrating security and privacy into the design phase of any new development ([Jacobsson, Boldt & Carlsson, 2015](#)). Impersonation, repeat, and related attacks are typical to OAuth. Work has been done to resolve these issues by incorporating another principle of Security Manager ([Emerson et al., 2015](#)). This Security Manager enhances security, availability, and efficiency by utilising a database recording the expiry time tokens, including other useful information to reduce various IoT network registrations and numerous IoT network logins.

Arno et al. developed the idea of engaging smart devices for securing assets and proposed a smart lock for bicycles using smartphones ([Arno, Toyoda & Sasase, 2015](#)). The central idea of this lock is an accelerometer-based authentication. Sample data is produced using the NFC, GPS, Bluetooth devices, and the idea is executed by using an Android-based smartphone ([Munch-Ellingsen et al., 2015](#)). User authentication is required when Cloud and IoT service providers need periodic access to IoT/Smart Devices for firmware upgrades and other routine maintenance ([Barreto et al., 2015](#)). The idea of using Dynamic

ID is quite active now, and a study is underway to secure IoT using Dynamic IDs ([Zhai et al., 2015](#); [Ilyas, Ali & Kueng, 2010](#)). The IoT mutual authentication system based on login ID, password hash, and MAC address along with the DBMS (Database Management System) for the management and logging of authorised and unauthorised access controls is proposed ([Devi et al., 2015](#)). Ruan et al. raised concerns about misuse of identity. Impersonation attacks are very popular in identity misuse. A random oracle framework is designed to counter the impersonation attack by widening the two-party conuration to the 'n' parties and developing an efficient two-party EAKA (explicit authentication key agreement) protocol as provided by the standard ([Ruan et al., 2015](#)) model.

Delegation-based IoT authentication is proposed in [Borgohain et al. \(2015\)](#) to resolve privacy concerns in IoT. The private mutual authentication model is introduced, which uses PKI encryption schemes to respond to privacy and security concerns using new protocols. The research introduced Identity-based Cryptography (IBC) and Elliptical Curve Cryptography (ECC) for end-to-end authentication. Asymmetric cryptography for end-to-end encryption ([Markmann, Schmidt & Wählisch, 2015](#)). Integrating Ciphering and Physical Authentication schemes is suggested for additional security, and 3rd-factor authentication Delegation-based IoT authentication is proposed in ([Borgohain et al., 2015](#)) to resolve privacy concerns in IoT. Authors have implemented this system using the open-source Vanadium framework ([Wu et al., 2016](#)). The research introduced Identity-based Cryptography (IBC) and Elliptical Curve Cryptography (ECC) for end-to-end authentication. Asymmetric cryptography for end-to-end encryption ([Markmann, Schmidt & Wählisch, 2015](#)). Integrating Ciphering and Physical Authentication schemes is suggested for further security and 3rd-factor authentication ([Crossman & Liu, 2015](#)). It is also highlighted that desirable security objectives can be obtained by providing Dynamic IDs-based authentication. The advanced framework for communicating multi-site knowledge with Ciphered Dynamic credential is also demonstrated in [Ilyas, Ali & Kueng \(2010\)](#). The IoT Continuous Authentication Protocol, where smart devices frequently communicate limited data/messages at short intervals, is proposed by Bamasag et al. The protocol is based on the Shamir secret sharing system, with the innovation of mutual authentication. Claimer Identity is checked using tokens provided for the same function ([Bamasag & Youcef-Toumi, 2015](#); [Crossman & Liu, 2015](#)). It is also highlighted that desirable security objectives can be obtained by providing Dynamic IDs-based authentication. The advanced framework for communicating multi-site knowledge with Ciphered Dynamic credential is also demonstrated in [Ilyas, Ali & Kueng \(2010\)](#). The IoT Continuous Authentication Protocol, where smart devices frequently communicate limited data/messages at short intervals, is proposed by Bamasag et al. The protocol is based on the Shamir secret sharing system, with the innovation of mutual authentication. Claimer Identity is checked using tokens provided for the same function ([Bamasag & Youcef-Toumi, 2015](#)). Developing modern protocols and integrating new features of IPV6 and 5G connectivity into IoT has been proposed by [Mahmoud et al. \(2015\)](#). The new word "Threat Index" is introduced to measure vulnerabilities in IoT and recommends the creation of new protection approaches for each layer of IoT ([Kumar, Vealey & Srivastava, 2016](#)). In the usage of IoT, the privacy of a person remains at risk. With the introduction of

smart technology, it is really important to take account of consumer safety. Often RFIDs are used for recognition purposes in IoT. The authors recommended the usage of IPsec along with RFID to protect user privacy. In this method, “Need to Know” dependent rule is implemented (Gross et al., 2015). Quick reply with IoT devices certainly improves every machine’s performance, but it again requires so much caution as suggested in (Condry & Nelson, 2016). A lightweight anonymous authentication protocol is recommended for an RFID-dependent authentication. In this technique, random tokens are created to preserve user privacy. It is claimed to protect consumer privacy, whereas cryptographic functions are neglected, which will face certain serious threats of misuse of RFIDs (Chen, Chen & Fang, 2017). Similarly, Díaz et al. implemented the Zero Information Authentication Protocol concept, along with several other authentication factors in IoT authentication. One time password (OTP) and Short Message Service (SMS) are two other variables that can be used for authentication (Díaz, Martín & Rubio, 2016), and (Jun, 2010). The session period plays a critical role in the system’s security. Authentication for a restricted period would exponentially impact systems’ security (Barrera et al., 2017). An important way is to handle authentication with restricted/limited information sharing or nil knowledge sharing as described in Coffey & Newe (1998). A new solution of hybrid cards (Swing-Pay) is presented, where a digital card unit comprising NFC and bio-metric authentication for peer-to-peer payments and identity management (Ghosh et al., 2017). Different forms of authentications are introduced to improve the process. Similarly, another Protocol (Pay-Cloak) (Majumder et al., 2017) to perform internet purchases using a bio-metric back cover for mobile phones has been suggested. Signature dependent authentication is indicated in Nishigori, Kawamoto & Sakurai (2017) where biometric grid reference points of an individual’s signature and the other behavioural characteristics of the human-being are analysed for secure authentication. These behavioural characteristics include writing pace, pen pressure on the paper, angle of the pen. Shoulder surfing attack and the availability of a printed copy of the user’s signature can dodge the scheme. Secure Authentication in Industrial IoT as proposed by Xiaoding et al. (2021) manages a user’s access to the blockchain as well as other applications. Another, very recent three-factor remote user authentication has been proposed by Patel et al. (2020) in which a record of authentication requests is controlled by an administrator or superuser. Rathee et al. (2020) proposed a graph-based social network model for forensic perspectives. Jiang et al. (2019) proposed an authentication protocol that uses an identity-based cryptosystem in which public key is used as the user’s identity, eliminates the need for certificates and simplifies network configuration, which is very useful for a common user instead of an administrator or superuser. Authentication and insider threat are crucial issues, and research is in progress where different methods are proposed and practised for securing an information system.

THE PROPOSED MODEL—VISTAS

A closed and confined environment is proposed where a digital fence in terms of IDS (Intrusion Detection System), and the IPS (Intrusion Prevention System) systems, are implemented to provide the information security of a mission-critical system. Much

research has been carried out to implement cybersecurity measures for physical threats from insiders, such as limited access, constant monitoring with close circuit cameras, and 24/7 surveillance by overlapping physical security personnel. Data transport is another critical issue where a man in the middle (MITM) attack can be used to steal data from insiders, and therefore protection must be carried out in this regard. Smart cryptography techniques for the secure distribution of larger data in cloud computing should be applied.

Access types

Different level access permissions are required to different levels and categories of the users. These can be categorised as follow:

Administrative Access:- Network operations, system administration & maintenance, backup & restore operations, database administration, and Data Transportation are such activities that are considered administrative activities and need escalated privileges.

User level Access or limited access:- Software usage, simple desk-work, printing, internet surfing are known as user activities that do not require escalated privileges than a standard user.

Experimental evaluation and environment setup

The proposed framework uses multi-factor authentication in a supervisory concept and multichain based blockchain for the immutable storage of access requests to mitigate the insider threat. For a Proof of Concept (POC), We have deployed VisTAS on a CentOS Server. The detail of the resources is as under.

Hardware Resources configured for the implementation and testing of the proposed VisTAS include a Dual Core CPU with 100 % Execution Capacity, 4 Gigabytes for Random Access Memory, 20 Gigabytes HDD for installation & storage, and a bridged network adopter.

Software Resources used to implement and test VisTAS in Linux using CentOS 8.0 x86_64 for the above-discussed hardware resources. Multichain 2.0.0 is used for blockchain implementation based on The Elliptic Curve Digital Signature Algorithm (ECDSA). We used Elasticsearch with Kibana in a Firefox 73.0.1 browser interface for storage and query of the data.

Implementation

Close circuit television cameras (CCTVs) are installed for physical monitoring and local login requests, and screen activities are also recorded using screen capturing applications. These activities are discussed in the following sections.

Operational sequence

This framework is covered in two different types of activities, i.e., Admin Activities and User Activities. Workflow and sequence of the activities are given in [Fig. 2](#) and enlisted as under.

- Administrator attempts to get the login to the server remotely using SSH (secure shell in Linux servers) and enters his/her ID and password.

- Server generates a random token, records it along with the request into a distributed ledger (DLT), and sends it to the supervisor/peer/colleague (as desired by the organization).
- Upon verification of the credentials, Requesting administrator is granted access to predefined resources/services.
- All the authentication credentials are recorded in a DLT and vet by the other peers.
- These entries are visible to peers and are being recorded in a DLT.

The contrast of standard authentication and additional authentication carried out by VisTAS is shown in [Fig. 3](#) and [Table 2](#) where a random code generator and blockchain has been introduced for visibility and transparency.

RESULTS AND DISCUSSION

Performance and security are two very important factors in a server's health. However, security becomes a critical objective that can supersede any performance matrix, and that's why sometimes we have to compromise on performance to achieve security. The effectiveness and workload of any framework or scheme can be obtained by monitoring the server on multiple parameters, especially the usage of processing power, IO activities, random access memory, network utilization, swap memory, and context switching. It is a win-win situation if the system/facility becomes deterrent/secure without compromising these performance matrices significantly. There are multiple application and system monitoring tools freely available, whereas System Activity Reports. Comparisons of these performance matrices are shown in the following graphs. SAR is one of the utilities being provided by "sysstat" which is a linux package bundled with other different utilities for system performance review. SAR utility can provide the following types of statistics to monitor and evaluate a system state.

- The overall CPU usage or workload
- Individualist CPU statistics
- Memory status (how much used and remaining available)
- Swap space status (used and available)
- I/O activities (System Wholesome)
- I/O activities (Individual Devices)
- Operating system statistics for context switching
- Load average and running queue data
- Statistics providing network status
- Specific interval report of SAR data

In this research, we used this utility to generate performance comparison on standard authentication viz-a-viz VisTAS based authentication. We focused on monitoring only important performance matrices like CPU Usage, Memory Usage, IO load, swap memory usage, context switching, process queue, and network traffic only.

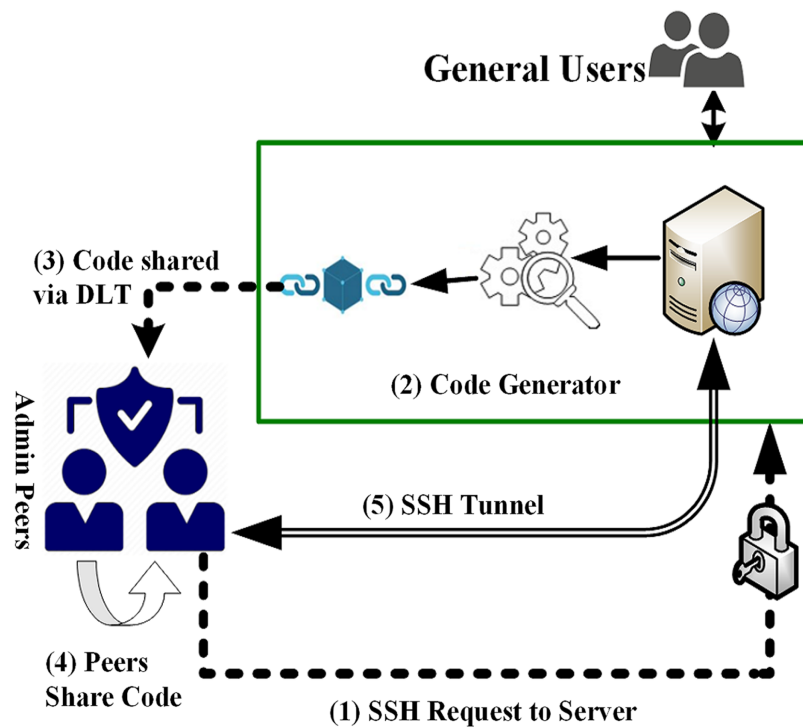


Figure 2 VisTAS—proposed authentication architecture.

Full-size [DOI: 10.7717/peerj-cs.516/fig-2](https://doi.org/10.7717/peerj-cs.516/fig-2)

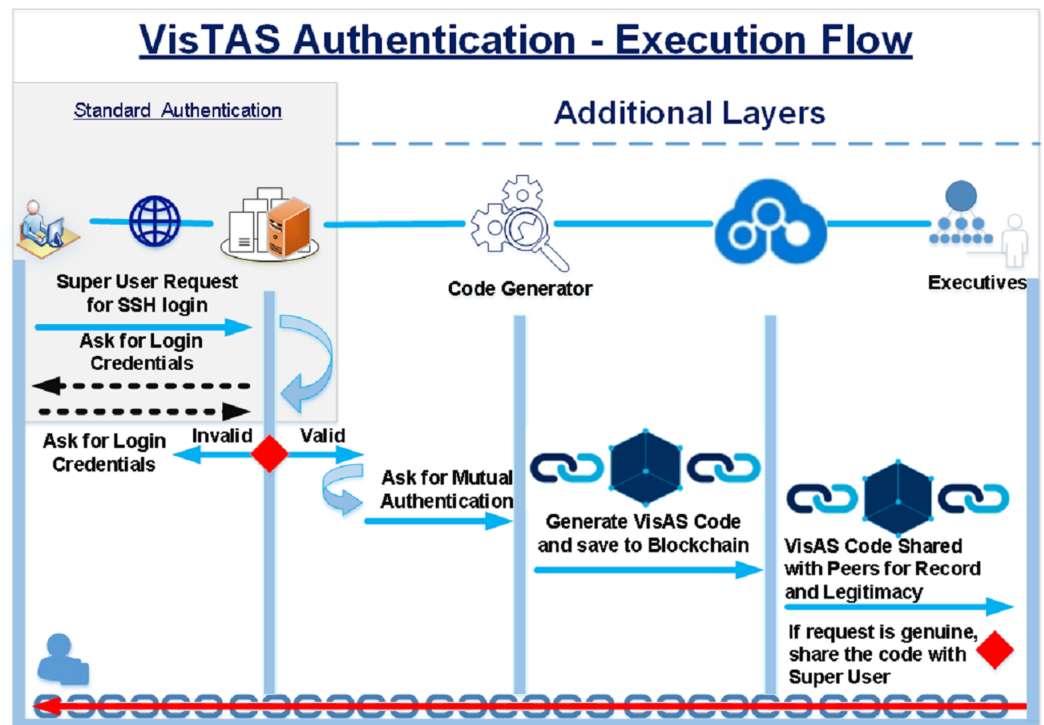


Figure 3 Execution flow of proposed architecture.

Full-size [DOI: 10.7717/peerj-cs.516/fig-3](https://doi.org/10.7717/peerj-cs.516/fig-3)

Table 2 A contrast of authentication schemes.

| Ser. | Parameter | Existing schemes | Proposed scheme |
|------|-------------------------|--|--|
| 1 | Confidentiality | Simple data transfer | Encrypted data transfer |
| 2 | Availability | Existing authentication schemes does not confirm availability | Our system provide higher fault tolerance in terms of availability by denying illegal requests |
| 3 | Immutability | Existing authentication schemes do not provide integration with blockchains | Proposed authentication scheme provides integration with blockchains |
| 4 | Traceability | Existing authentication schemes have no traceability mechanism using immutable data structures i.e., blockchains | Proposed scheme store traceable data in blockchains to provide immutability |
| 5 | Speed | Data transmission occure at the network speed | A very negligible transmission delay may occure while storing data in the blockchain |
| 6 | Transparency/visibility | Peers and other members have to visibility on the authentication system | Peers have access on the blockchain streams to view data and allow and validate authentication |
| 7 | Mutual Authentication | No practice of mutual authentication | Mutual authentication is carried out using two men rule |

Complexity and efficiency

The most important segment of VisTAS is storing data in a blockchain which is carried through APIs. As discussed in the previous section, VisTAS used “Multichain”, and these APIs have a time complexity of $O(\log(n))$, where n is the number of items being stored or retrieved ([Multichain, 2019](#)). APIs use index lookups in retrieving a data block and any general index has a complexity of $O(\log(n))$. The efficiency and processing impact of the proposed model is covered in subsequent sections.

I/O load analysis

Input-Output (I/O) workload has a significant impact on the performance of a computing system. The following parameters can be used to evaluate I/O overhead using SAR in the context of I/O and transfer rate statistics. VisTAS requires additional overhead for data input and processing for additional security.

- **tps** The total number of transfers issued per second to physical devices. A transfer is a request for an I/O to a physical device. Multiple logical requests can be merged and treated as a single device I/O request. The data transfer can be of an undetermined volume.
- **rtps** The total number of reading requests to physical devices issued per second.
- **wtps** The total number of write requests issued to physical devices per second.
- **bread/s** The total volume of data read received the devices in blocks per second. Blocks are equivalent to sectors with 2.4 and newer kernels; therefore have a size of 512 bytes. With older kernels, the block is of an undetermined size.
- **bwrtn/s** The total amount of data written to devices in blocks per second.

I/O overhead shown by the SAR statistics using the VisTAS as compared to the standard is shown in [Fig. 4](#).

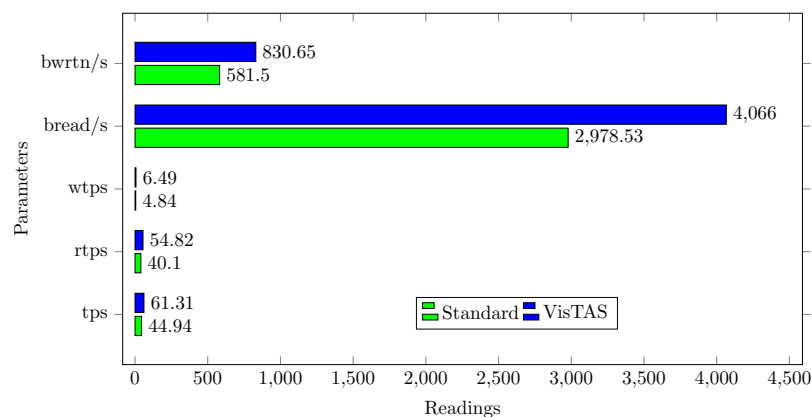


Figure 4 I/O load comparison.

Full-size  DOI: 10.7717/peerj-cs.516/fig-4

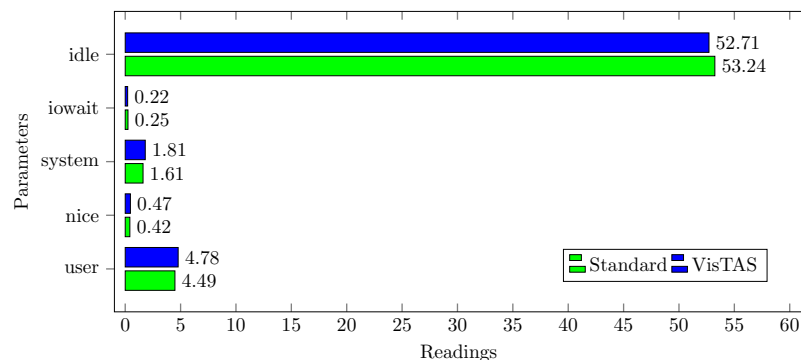


Figure 5 CPU usage.

Full-size  DOI: 10.7717/peerj-cs.516/fig-5

CPU usage analysis

CPU usage analysis return the statistics for the following:

- **%usr:** The utilisation of the CPU in terms of percentage occurred during the execution of a user-level application.
- **%nice** The utilisation in percentage that occurred during the execution of a user-level application with nice priority.
- **%system** The CPU utilisation percentage that occurred in the execution of a system level (kernel) activity which also includes the time spent in servicing the hardware and software interrupts.
- **%sys** The CPU utilisation in percentage that occurred while running at the system level (kernel) excluding time spent on the hardware or software-based interrupts.
- **%iowait** The percentage of the time that a CPU or CPUs were idle during which the system had an exceptional I/O disk request.

By analysing the graph shown in Fig. 5, processing impact is very minute while using VisTAS compared to standard authentication.

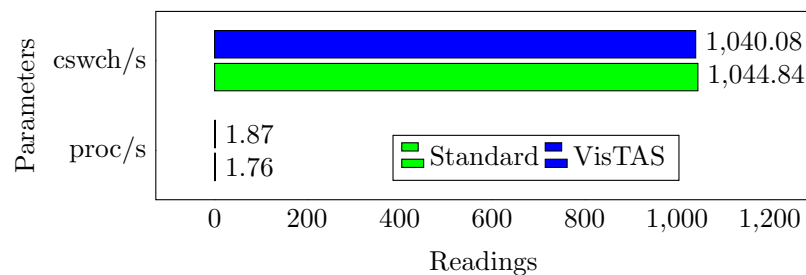


Figure 6 Context switching.

Full-size DOI: [10.7717/peerj-cs.516/fig-6](https://doi.org/10.7717/peerj-cs.516/fig-6)

Context switching analysis

Context Switching leads to an additional workload associated with sharing the device cache for various tasks, running the scheduler. Context switching among the threads of the same application or process is faster than different processes. Its overhead can be observed by the process created per unit of time and the number of context switches that occurred per second as follows, and the comparison is shown in Fig. 6.

- **proc/s.** The total number of tasks created in a unit time.
- **cswch/s.** The total number context switches occurred in a unit time.

Process queue analysis

Statistics showing the length of the system process's queue and load averages determine the system's efficiency. The following can be used to check the system's health and performance:

- **runq-sz.** This shows the number of tasks waiting for the CPU.
- **plist-sz.** Returns the total number of the tasks present in the task list.
- **ldavg-1.** Returns the last-minute average load.
- **ldavg-5.** Returns the average system load for 5 min.
- **ldavg-15.** Returns the average system load for last 15 min.

The impact of VisTAS on process queue management compared to standard authentication as depicted in Fig. 7 is negligible.

Network traffic analysis

- **rxpck/s.** Shows total number of packets received in unit time.
- **txpck/s.** Shows total number of packets transmitted in unit time.
- **rxkB/s.** Shows data volume in kilobytes received in unit time.
- **txkB/s.** Shows data volume in kilobytes transmitted in unit time.
- **rxcmp/s.** Shows compressed packets count received per second (for cslip etc.).
- **txcmp/s.** Shows compressed packets count transmitted per second.
- **rxmcst/s.** Shows multi-cast packets count received per second.

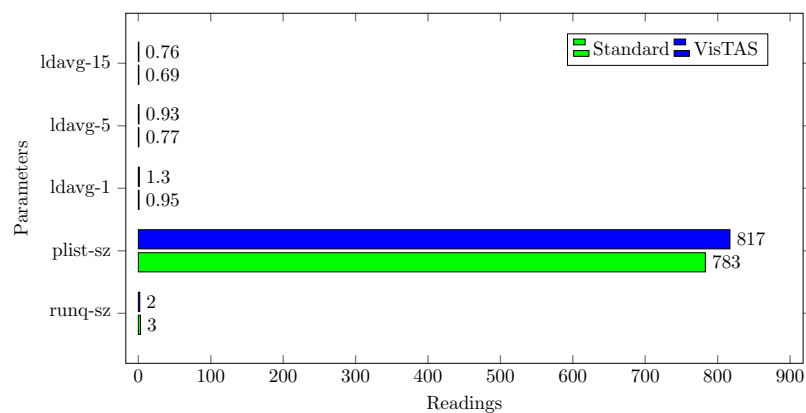


Figure 7 Queue impact.

Full-size DOI: 10.7717/peerj-cs.516/fig-7

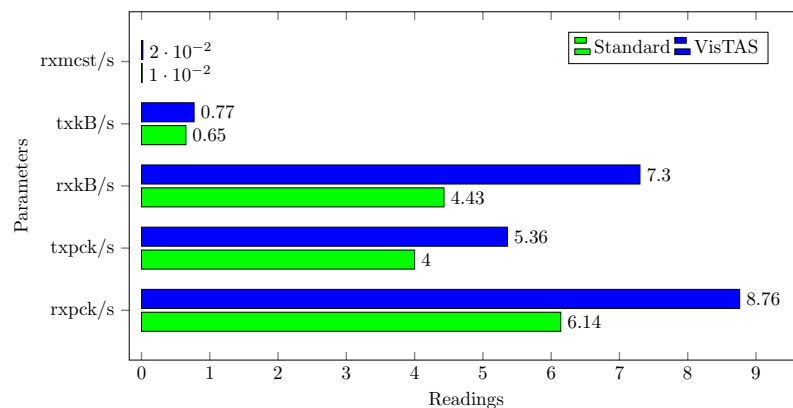


Figure 8 Network load analysis.

Full-size DOI: 10.7717/peerj-cs.516/fig-8

While comparing network load between VisTAS and standard authentication as shown in Fig. 8, it observed a difference of two to three packets for an authentication activity.

Swap memory usage analysis

Swap memory extends system memory. The utilisation of this memory is also used to monitor the system's performance. Important attributes to monitor swap memory are as follows.

- **kbswpfree.** Free swap space available in kilobytes.
- **kbswpused.** Used/Occupied swap space in kilobytes.
- **%swpused.** Percentage of used swap space.
- **kbswpcad.** Cached swap memory in kilobytes. This is the memory swapped out earlier and is swapped back in but still also in the swap area.
- **%swpcad.** Percentage of cached swap memory in relation to the amount of used swap space.

Figure 9 has shown the swap memory impact comparison between VisTAS and standard authentication and ignore-able difference found in swap memory utilization.

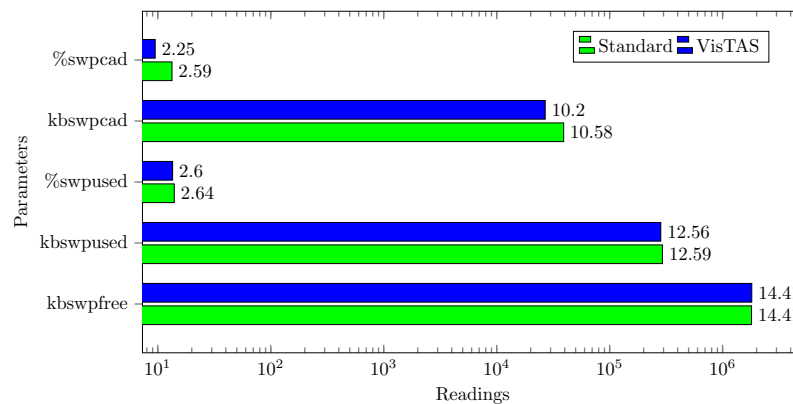


Figure 9 Swap memory load.

Full-size DOI: 10.7717/peerj-cs.516/fig-9

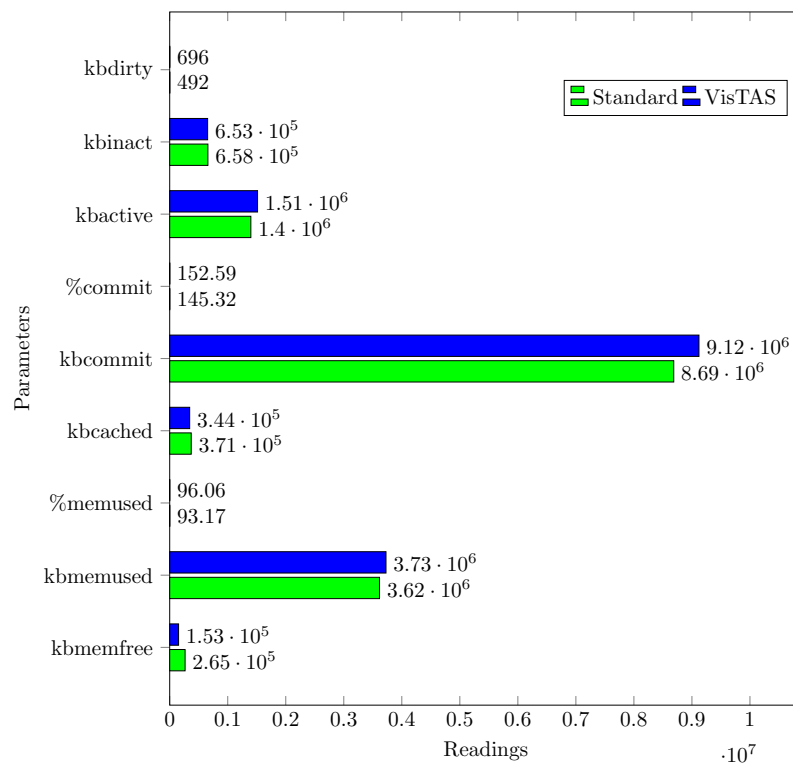


Figure 10 Overall memory usage.

Full-size DOI: 10.7717/peerj-cs.516/fig-10

Memory usage analysis

Memory usage analysis is carried out as shown in Fig. 10 in terms of the following:

- **kbmemfree.** Available free memory (kilobytes).
- **kbmemused.** memory used (kilobytes). Excluding the memory kernel itself used.
- **%memused.** Used memory in percentage.
- **kbbuffers.** Buffer memory used by the kernel in kilobytes.
- **kbcached.** Cache memory used by the kernel in kilobytes.

- **kbcommit.** Memory needed for the current workload (kilobytes). An estimate of how much RAM/swap is required to guarantee that system never goes out of memory.
- **%commit** Memory percentage required for the current workload in relation to the total memory volume (RAM+swap).

The memory usage graph shows the difference in memory consumption of VisTAS and the standard system. VisTAS generates dynamic codes and uses distributed ledger application, which is highlighted as slightly extra memory usage.

Results summary

A comparison graph of these performance matrices is depicted in [Fig. 11](#). By evaluating and analyzing these values, we have achieved deterrence, peer control, visibility over the remote authentications, and immutable record of login requests.

SWOT ANALYSIS

Linux is a well-known OS rendering various servers and cloud services. It has different flavours, including Redhat, Ubuntu, CentOS, Fedora, SUSE and Oracle Linux, etc. CentOS (Community Enterprise Operating System) and Oracle Linux servers are Redhat extensions. For the implementation of the VisTAS, on the server-side, freely available open-source CentOS Server 8.0, 86_64 Operating System and for distributed ledgers and immutability, we commissioned Multichain ([Multichain, 2019](#)), which is an open-source implementation of the bitcoin protocol. On the client-side, we used command-line applications like Linux terminal and putty. Linux provides Plug-able Authentication Module (PAM) to implement an identification and authentication framework. VisTAS exploited this functionality positively to provide mutual authentication, as shown in [Fig. 3](#).

The proposed model provided a mechanism for remote authentication, which has its good and bad. Based on the graph presenting the overall impact of VisTAS [Fig. 11](#) as discussed earlier in previous sections, SWOT analysis [Fig. 12](#) is used to analyse and highlight the good and the bad. The proposed model provides 4Ds out of the well-known 5Ds of Security, i.e., Deter, Detect, Delay, Deny and Defend.

Strengths

Deterrence, Delay, Deny and Defend are the strengths of the proposed model. Deterrence is spelt out by providing visibility to the peers and recording authentication data to the blockchain. The delay factor is achieved by getting peer permission for authentication. The peer can deny authentication if she smells some insider threat, and overall, the defence is achieved by rejecting all the illegal authentication requests.

Weaknesses

The system has to face some extra processing workload of blockchain and dynamic key transfer. Similarly, communication delay may also occur in peak working hours where network congestion may delay the legitimate requests and remote administrative operation or activity can not be performed in case of communication blackout.

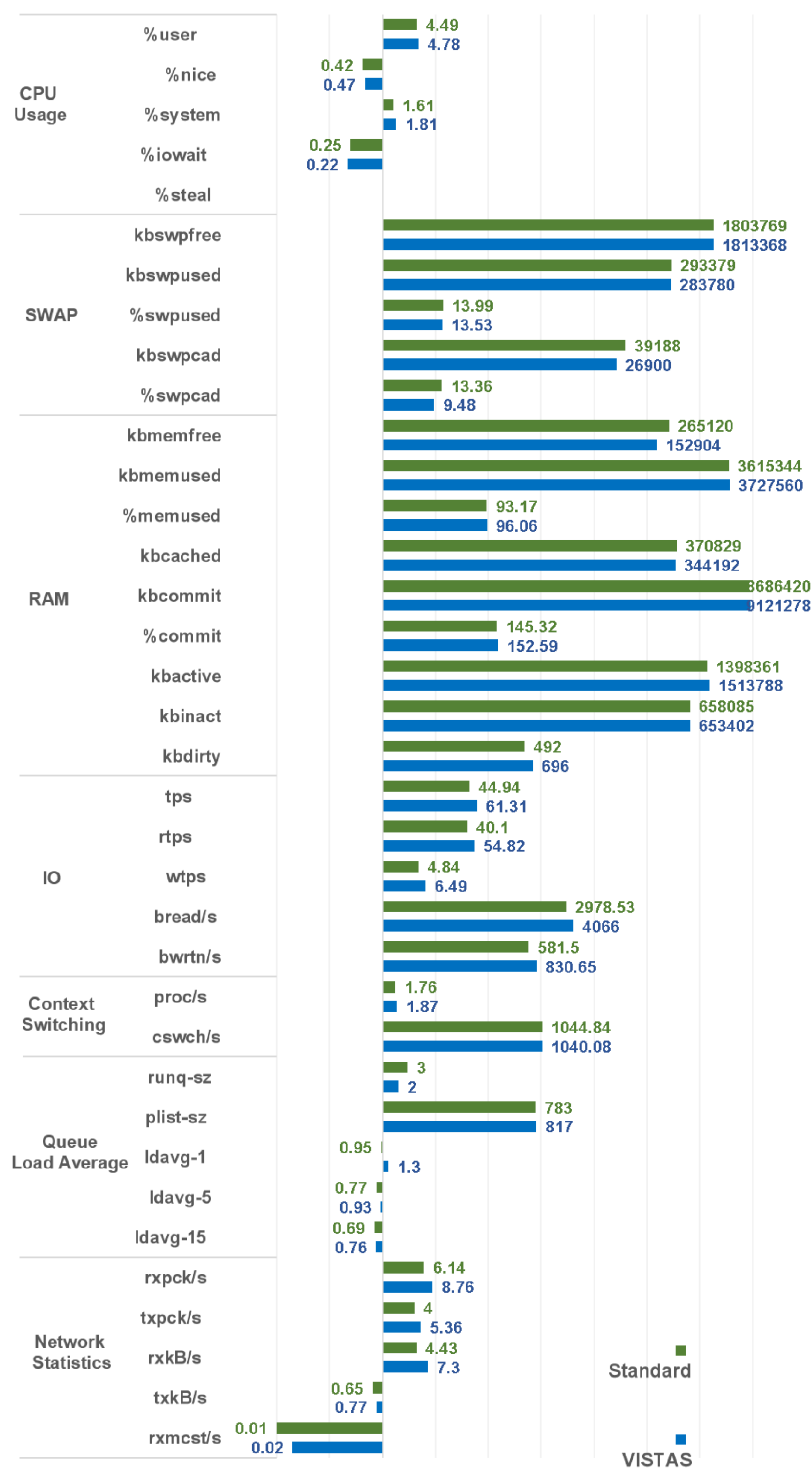


Figure 11 Overall SAR analysis of the VisTAS.

Full-size DOI: 10.7717/peerj-cs.516/fig-11

STRENGTHS

- ✓ Deterrence
- ✓ Supervised Authentication
- ✓ Peer Control
- ✓ Visible Access
- ✓ Distributed Ledger based immutable data storage

OPPORTUNITIES

- ✓ Immutable remote authentication data availability for analysis
- ✓ Insiders threat analysis

WEAKNESSES

- ✓ Extra workload
- ✓ Communication delay
- ✓ Only for remote SSH authentication
- ✓ No remote operation in communication blackout
- ✓ Redundant Resources may be required

Threats

- ✓ Peer Compromise
- ✓ Amenable to mollification



Figure 12 SWOT analysis of the proposed scheme.

Full-size DOI: 10.7717/peerj-cs.516/fig-12

Opportunities

Detection of insider threat is possible only if legitimate data of authentication schemes are available. Using this scheme, we can analyse this data to detect the insider and achieve the 5th “D” of security.

Threats

Peers and stakeholders are equally responsible for the success of any security system. In this scheme, peers are actively involved and may pose some threat of blackmailing or unavailability of services.

Results summary and discussion

This framework’s effectiveness and workload are obtained by monitoring the server on multiple parameters, especially the usage of processing power, I/O activities, Random Access Memory (RAM), network utilisation, swap memory, and context switching. It is a win-win situation if the system/facility becomes deterrent/secure without compromising these performance matrices significantly. There are multiple application and system monitoring tools freely available, like System Activity Reports (SAR) in Linux. Comparisons of these performance matrices are discussed in the following paragraphs.

This research used the SAR utility to generate performance comparison on standard authentication viz-a-viz VisTAS based authentication. We focused on monitoring only necessary performance matrices like CPU usage, memory usage, I/O load, swap memory usage, context switching, process queue, and network traffic only.

I/O Analysis: The Input-Output (I/O) overhead significantly affects the performance of a system. SAR statistics in terms of I/O and transfer rate shows marginal overhead.

CPU Usage Analysis: By analysing the graph’s values, the processing impact is very minute while using VisTAS compared to standard authentication.

Context Switching Analysis: The Context Switching leads to an extra workload due to sharing the system cache among multiple tasks and running the scheduler etc. Context switching between threads of the same application or process is faster than among different processes. Its overhead can be monitored by processes created in a per unit of time, and the number of context switching occurred per second as following.

Process Queue Analysis: Statistics showing the length of the system process's queue and load average determine the system's efficiency. The following can be used to check the system's health and performance: The impact of VisTAS on process queue management compared to standard authentication as depicted in queue-management is negligible.

Network Traffic Analysis: While comparing network load between VisTAS and standard authentication, as shown in network load, it observed a difference of two to three packets for an authentication activity.

Swap Memory Usage Analysis: Swap memory extends system memory. The utilisation of this memory is also used to monitor the system's performance. Swap memory load shows the swap memory impact comparison between VisTAS and standard authentication and ignore-able difference found swap memory utilisation. The memory usage graph shows the difference in memory consumption of VisTAS vs standard system. VisTAS generates dynamic codes, uses a distributed ledger application, and consumes slightly extra memory, which is highlighted in the swap memory usage analysis graph in [Fig. 9](#).

CONCLUSION & FUTURE WORK

Insider threats are of primary concern for all types of organizations. Extensive research has been carried out in this domain of information security. The deterrence perspective is missing for insiders in information security because of their specialised privileges to the system resources. Insider threat mitigation strategies in the dimensions of the social, behavioural, and technical arena are explored.

Shared Secret, any two of three and two men rule, etc., have already been used and practised for a long time in physical security measures such as physical locks for significant and critical sites. Implementing the two-person rule would strengthen the information system's protection and visibility in its operations by authenticating and validating respective stakeholders' activities. This paper suggested a two-person approach with a supervisory concept for authentication and validation of user activities. A pre-arranged scenario is also discussed with a view to practice this system. The system should therefore deal with increased processing due to the blockchain utilisation and dynamic key transfer. Similarly, during peak working hours, network congestion may cause legitimate requests to get delayed. In the case of a communication blackout, remote administrative operations or activities cannot be performed.

Implementation of VisTAS revealed that specifically for mission-critical environments like data centres/Supervisory Control and Data Acquisition Systems (SCADA), the framework is quite effective and renders a practical approach. Performance evaluation of VisTAS shows satisfactory and competitive results. In the future, a rigorous assessment is

planned in which stress tests will be carried out by deploying the framework into some large-scale environment for validation purposes.

We have implemented VisTAS in a test-bed of the Linux environment, and its performance has been evaluated using SAR. According to the results depicted by SAR, additional processing is required for extra security. In our future work, we will implement this framework in a suitable open-source Operating System to facilitate the implementation of the proposed framework and find interlinking user activities through some graph databases.

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

This research has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 801522, by Science Foundation Ireland and co-funded by the European Regional Development Fund through the ADAPT Centre for Digital Content Technology grant number 13/RC/2106_P2. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Grant Disclosures

The following grant information was disclosed by the authors:
European Union's Horizon: 801522.
Science Foundation Ireland.
European Regional Development Fund: 13/RC/2106_P2.

Competing Interests

The authors declare that they have no competing interests.

Author Contributions

- Ahmad Ali conceived and designed the experiments, performed the experiments, analyzed the data, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the paper, and approved the final draft.
- Mansoor Ahmed conceived and designed the experiments, performed the experiments, analyzed the data, performed the computation work, authored or reviewed drafts of the paper, and approved the final draft.
- Abid Khan performed the experiments, analyzed the data, performed the computation work, prepared figures and/or tables, and approved the final draft.
- Adeel Anjum analyzed the data, authored or reviewed drafts of the paper, and approved the final draft.
- Muhammad Ilyas performed the experiments, analyzed the data, prepared figures and/or tables, authored or reviewed drafts of the paper, and approved the final draft.
- Markus Helfert performed the computation work, authored or reviewed drafts of the paper, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

Code and instructions are available in a [Supplemental File](#).

Supplemental Information

Supplemental information for this article can be found online at <http://dx.doi.org/10.7717/peerj-cs.516#supplemental-information>.

REFERENCES

- Ahmad MB, Fahad M, Khan AW, Asif M. 2016.** A first step towards reducing insider threats in government organizations. *International Journal of Computer Science and Network Security (IJCSNS)* **16**(6):81.
- Ali A, Ahmed M, Imran M, Khattak HA. 2020.** Security and privacy issues in fog computing. In: *Fog Computing: Theory and Practice*. 105–137.
- Ali A, Khan A, Ahmed M, Jeon G. 2021.** BCALS: Blockchain-based secure log management system for cloud computing. *Transactions on Emerging Telecommunications Technologies* e4272.
- Arno A, Toyoda K, Sasase I. 2015.** Accelerometer assisted authentication scheme for smart bicycle lock. In: *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. Piscataway: IEEE, 520–523.
- Bamasag OO, Youcef-Toumi K. 2015.** Towards continuous authentication in internet of things based on secret sharing scheme. In: *Proceedings of the WESS'15: Workshop on Embedded Systems Security*. New York: ACM, 1.
- Barrera D, Chuat L, Perrig A, Reischuk RM, Szalachowski P. 2017.** The scion internet architecture. *Communications of the ACM*. **60**(6):56–65.
- Barreto L, Celesti A, Villari M, Fazio M, Puliafito A. 2015.** An authentication model for iot clouds. In: *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015*. Piscataway: IEEE, 1032–1035.
- Bera B, Saha S, Das AK, Kumar N, Lorenz P, Alazab M. 2020.** Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment. *IEEE Transactions on Vehicular Technology* **69**(8):9097–9111 DOI [10.1109/TVT.2020.3000576](https://doi.org/10.1109/TVT.2020.3000576).
- Bhardwaj A, Shah SBH, Shankar A, Alazab M, Kumar M, Gadekallu TR. 2020.** Penetration testing framework for smart contract blockchain. *Peer-to-Peer Networking and Applications* **5**(2):1–16 DOI [10.1007/s12083-020-00991-6](https://doi.org/10.1007/s12083-020-00991-6).
- Bisong A, Rahman M. 2011.** An overview of the security concerns in enterprise cloud computing. Available at <https://arxiv.org/abs/1101.5613>.
- Borgohain T, Borgohain A, Kumar U, Sanyal S. 2015.** Authentication systems in internet of things. arXiv. Available at <https://arxiv.org/abs/1502.00870>.
- Bou-Harb E, Lucia W, Forti N, Weerakkody S, Ghani N, Sinopoli B. 2017.** Cyber meets control: a novel federated approach for resilient cps leveraging real cyber threat intelligence. *IEEE Communications Magazine* **55**(5):198–204 DOI [10.1109/MCOM.2017.1600292CM](https://doi.org/10.1109/MCOM.2017.1600292CM).
- Bunn M, Sagan SD. 2017.** A worst practices guide to insider threats: lessons from past mistakes. *Language Magazine* **3**:1.
- Chen M, Chen S, Fang Y. 2017.** Lightweight anonymous authentication protocols for rfid systems. *IEEE/ACM Transactions on Networking* **25**(3):1475–1488 DOI [10.1109/TNET.2016.2631517](https://doi.org/10.1109/TNET.2016.2631517).

- Chowdhury MJM, Ferdous MS, Biswas K, Chowdhury N, Kayes A, Alazab M, Watters P. 2019.** A comparative analysis of distributed ledger technology platforms. *IEEE Access* 7:167930–167943 DOI 10.1109/ACCESS.2019.2953729.
- Coffey T, Neue T. 1998.** Realisation of a minimum-knowledge identification and signature scheme. *Computers & Security* 17(3):253–264 DOI 10.1016/S0167-4048(98)80339-8.
- Condry MW, Nelson CB. 2016.** Using smart edge iot devices for safer, rapid response with industry iot control operations. *Proceedings of the IEEE* 104(5):938–946 DOI 10.1109/JPROC.2015.2513672.
- Crossman MA, Liu H. 2015.** Study of authentication with iot testbed. In: *2015 IEEE International Symposium on, Technologies for Homeland Security (HST)*. Piscataway: IEEE, 1–7.
- Deepa N, Pham Q-V, Nguyen DC, Bhattacharya S, Gadekallu TR, Maddikunta PKR, Fang F, Pathirana PN. 2020.** A survey on blockchain for big data: approaches, opportunities, and future directions. arXiv. Available at <https://arxiv.org/abs/2009.00858>.
- Devi GU, Balan EV, Priyan M, Gokulnath C. 2015.** Mutual authentication scheme for iot application. *Indian Journal of Science and Technology* 8(26):1–5.
- Díaz M, Martn C, Rubio B. 2016.** State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer Applications* 67:99–117.
- Emerson S, Choi Y-K, Hwang D-Y, Kim K-S, Kim K-H. 2015.** An oauth based authentication mechanism for iot networks. In: *2015 International Conference on, Information and Communication Technology Convergence (ICTC)*. Piscataway: IEEE, 1072–1074.
- Farooq M, Waseem M, Khairi A, Mazhar S. 2015.** A critical analysis on the security concerns of internet of things (iot). *International Journal of Computer Applications* 111(7):1–6.
- Fischer EA. 2014.** Cybersecurity issues and challenges: in brief. In: *Congressional Research Service*.
- Flynn L, Huth C, Trzeciak R, Buttles P. 2013.** Best practices against insider threats in all nations. Technical report, Pittsburgh: Software Engineering Institute.
- Ghosh S, Majumder A, Goswami J, Kumar A, Mohanty SP, Bhattacharyya BK. 2017.** Swing-pay: one card meets all user payment and identity needs: a digital card module using nfc and biometric authentication for peer-to-peer payment. *IEEE Consumer Electronics Magazine* 6(1):82–93 DOI 10.1109/MCE.2016.2614522.
- Gross H, Hölbl M, Slamanig D, Spreitzer R. 2015.** Privacy-aware authentication in the internet of things. In: *International Conference on Cryptology and Network Security*. Berlin: Springer, 32–39.
- Homoliak I, Toffalini F, Guarnizo J, Elovici Y, Ochoa M. 2019.** Insight into insiders and it: a survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)* 52(2):30 DOI 10.1145/3303771.
- Ilyas M, Ali A, Kueng J. 2010.** Websea: a secure framework for multi-site knowledge representation in software engineering. In: *International Conference on Bio-Inspired Models of Network, Information, and Computing Systems*. Berlin: Springer, 682–686.
- Jacobsson A, Boldt M, Carlsson B. 2015.** A risk analysis of a smart home automation system. *Future Generation Computer Systems* 56:719–733 DOI 10.1016/j.future.2015.09.003.
- Jeong H-DJ, Lee W, Lim J, Hyun W. 2015.** Utilizing a bluetooth remote lock system for a smartphone. *Pervasive and Mobile Computing* 24:150–165 DOI 10.1016/j.pmcj.2015.07.010.
- Jiang X, Liu M, Yang C, Liu Y, Wang R. 2019.** A blockchain-based authentication protocol for wlan mesh security access. *Computers, Materials & Continua* 58(1):45–59 DOI 10.32604/cmc.2019.03863.

- Jouini M, Rabai LBA, Aissa AB. 2014.** Classification of security threats in information systems. *Procedia Computer Science* 32:489–496 DOI 10.1016/j.procs.2014.05.452.
- Jun BLJ. 2010.** Implementing zero-knowledge authentication with zero knowledge (zka wz). *Python Papers Monograph* 2:1–19.
- Kandias M, Virvilis N, Gritzalis D. 2011.** The insider threat in cloud computing. In: *International Workshop on Critical Information Infrastructures Security*. Berlin: Springer, 93–103.
- Kumar SA, Vealey T, Srivastava H. 2016.** Security in internet of things: challenges, solutions and future directions. In: *2016 49th Hawaii International Conference on System Sciences (HICSS)*. Piscataway: IEEE, 5772–5781.
- Langner R. 2011.** Stuxnet: dissecting a cyberwarfare weapon. *IEEE Security & Privacy* 9(3):49–51 DOI 10.1109/MSP.2011.67.
- Mahmoud R, Yousuf T, Aloul F, Zualkernan I. 2015.** Internet of things (iot) security: current status, challenges and prospective measures. In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. Piscataway: IEEE, 336–341.
- Majumder A, Goswami J, Ghosh S, Shrivastawa R, Mohanty SP, Bhattacharyya BK. 2017.** Pay-cloak: a biometric back cover for smartphones: facilitating secure contactless payments and identity virtualization at low cost to end users. *IEEE Consumer Electronics Magazine* 6(2):78–88 DOI 10.1109/MCE.2016.2640739.
- Markmann T, Schmidt TC, Wählisch M. 2015.** Federated end-to-end authentication for the constrained internet of things using ibc and ecc. *ACM SIGCOMM Computer Communication Review* 45(4):603–604 DOI 10.1145/2829988.2790021.
- Markóczy L. 2003.** Trust but verify: distinguishing distrust from vigilance. In: *Academy of Management Conference*.
- Masdari M, Ahmadzadeh S. 2017.** A survey and taxonomy of the authentication schemes in telecare medicine information systems. *Journal of Network and Computer Applications* 87:1–19 DOI 10.1016/j.jnca.2017.03.003.
- Multichain. 2019.** Multichain implementation. Available at <https://www.multichain.com/> (accessed 25 August 2019).
- Munch-Ellingsen A, Karlsen R, Andersen A, Akselsen S. 2015.** Two-factor authentication for android host card emulated contactless cards. In: *2015 First Conference on, Mobile and Secure Services (MOBISECSERV)*. Piscataway: IEEE, 1–6.
- Nishigori T, Kawamoto J, Sakurai K. 2017.** Improving the accuracy of signature authentication using the eight principles of yong. In: *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*. New York: ACM, 32.
- Patel C, Joshi D, Doshi N, Veeramuthu A, Jhaveri R. 2020.** An enhanced approach for three factor remote user authentication in multi-server environment. *Journal of Intelligent & Fuzzy Systems* 39(6):1–12.
- Rathee G, Garg S, Kaddoum G, Jayakody DNK, Piran J, Muhammad G. 2020.** A trusted social network using hypothetical mathematical model and decision-based scheme. *IEEE Access* 9:4223–4232.
- Ruan O, Kumar N, He D, Lee J-H. 2015.** Efficient provably secure password-based explicit authenticated key agreement. *Pervasive and Mobile Computing* 24:50–60 DOI 10.1016/j.pmcj.2015.06.008.
- Schlicher BG, MacIntyre LP, Abercrombie RK. 2016.** Towards reducing the data exfiltration surface for the insider threat. In: *2016 49th Hawaii International Conference on, System Sciences (HICSS)*. Piscataway: IEEE, 2749–2758.

- Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. 2015. Security, privacy and trust in internet of things: the road ahead. *Computer Networks* 76:146–164 DOI 10.1016/j.comnet.2014.11.008.
- Silowash G, Cappelli D, Moore A, Trzeciak R, Shimeall TJ, Flynn L. 2012. Common sense guide to mitigating insider threats 4th edition. Technical report, DTIC Document. Pittsburg: Carnegie-mellon Univ Pittsburgh Pa Software Engineering Inst.
- Singh S, Hosen AS, Yoon B. 2021. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access* 9:13938–13959.
- Singh S, Sharma PK, Yoon B, Shojafar M, Cho GH, Ra I-H. 2020. Convergence of blockchain and artificial intelligence in iot network for the sustainable smart city. *Sustainable Cities and Society* 63(10):102364 DOI 10.1016/j.scs.2020.102364.
- Theoharidou M, Kokolakis S, Karyda M, Kiountouzis E. 2005. The insider threat to information systems and the effectiveness of iso17799. *Computers & Security* 24(6):472–484 DOI 10.1016/j.cose.2005.05.002.
- van der Haar D. 2015. Canvis: a cardiac and neurological-based verification system that uses wearable sensors. In: *2015 Third International Conference on, Digital Information, Networking, and Wireless Communications (DINWC)*. Piscataway: IEEE, 99–104.
- Wang D, He D, Wang P, Chu C-H. 2015. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. *IEEE Transactions on Dependable and Secure Computing* 12(4):428–442 DOI 10.1109/TDSC.2014.2355850.
- Wang J, Chen W, Wang L, Ren Y, Sherratt RS. 2020. Blockchain-based data storage mechanism for industrial internet of things. *Intelligent Automation and Soft Computing* 26(5):1157–1172 DOI 10.32604/iasc.2020.012174.
- Wu DJ, Taly A, Shankar A, Boneh D. 2016. Privacy, discovery, and authentication for the internet of things. arXiv. Available at <https://arxiv.org/abs/1604.06959>.
- Xiaoding W, Garg S, Lin H, Jalilpiran M, Hu J, Hossain MS. 2021. Enabling secure authentication in industrial iot with transfer learning empowered blockchain. *IEEE Transactions on Industrial Informatics*. Piscataway: IEEE.
- Yusop ZM, Abawajy J. 2014. Analysis of insiders attack mitigation strategies. *Procedia-Social and Behavioral Sciences* 129:581–591 DOI 10.1016/j.sbspro.2014.03.716.
- Zhai J, Cao T, Chen X, Huang S. 2015. Security on dynamic id-based authentication schemes. *International Journal of Security and its Applications* 9(1):387–396 DOI 10.14257/ijisia.2015.9.1.37.